https://doi.org/10.51483/IJDSBDA.1.2.2021.14-22 ISSN: 2710-2599

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Data Science and Big Data Analytics

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper **Open Access**

Data protection in a European world of ideals: An unforeseeable division of camps

Heather Taylor[1*]

[1]Trinity College, Dublin, The University of Dublin, Ireland. E-mail: taylorhe@tcd.ie

Article Info

Volume 1, Issue 2, May 2021
Received : 24 February 2021
Accepted : 18 April 2021
Published : 05 May 2021
doi: 10.51483/IJDSBDA.1.2.2021.14-22

Abstract

The right to the protection of personal data has taken on a whole new meaning in the technological rebirth of the New Age movement. We are no longer a name and a number; we are an amalgamation of the many digital personalities we both wittingly and unintentionally create online. This ability to "create information about data that were never apparent or intended in the source information" is, nonetheless, yin and yang. What's more, such repurposing undermines the right to informational self-determination, by virtue of which individuals should be able to consent to how and if their personal data should be processed, especially when combined. It remains that the rights to privacy and to the protection of personal data are not absolute. Mass collection and treatment of multiple-source data sets are undeniably indispensable in certain contexts: this is especially true as regards government surveillance in the fight against terrorism and organized crime. The question is, therefore, in what circumstances and to what extent may boundaries be imposed on these state authorities? This article explores the rise in so-called "big data applications," and how the two most instrumental courts in Europe as regards human rights and freedoms are shaping the future of data protection in Europe, albeit their paths are starting to diverge.

Keywords: *Data protection, ECHR, CJEU, targeted processing, big data, communications data, personal data, terrorism, safeguards, automated processing*

1. Introduction

The right to the protection of personal data is to be considered in respect of its place in society.[1] If we are to go by the findings of one report, according to which "we are no longer judged on the basis of our actions, but on the basis of what all the data about us indicate our probable actions may be,"[2] it would be fair to say that its place is center stage.

Although not explicitly consecrated as such in the ECHR,[3] the right to personal data protection has been assimilated by the broad notion that is the right to respect for one's private life.[4] On the other hand, the right to personal data protection is recognized as such,[5] distinct from the right to privacy,[6] within the legal order of the European Union.

1 Council of Europe, Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [2018] CETS No 108 (Convention 108+), Preamble; Case C 311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Schrems* [2020] ECLI:EU:C:2020:559, para 172.

2 Norwegian Data Protection Authority (*Datatilsynet*), 'Big data - privacy principles under pressure' (2013), 7, para 8.

3 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14 [1950] ETS 5.

4 Article 8 ECHR. See for example *S and Marper v The UK* App nos 30562/04 and 30566/04 [2008] ECHR 1581, paras 66-67.

5 Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (EU Charter), Article 8.

6 *Ibid*. Article 7.

* *Corresponding author: Heather Taylor, Trinity College, Dublin, The University of Dublin, Ireland. E-mail: taylorhe@tcd.ie*

In essence, personal data[7] is protected from processing, i.e., "any operation or set of operations" performed upon it, starting with its collection.[8]

For society, the advantages of exploiting personal data can be exemplified in 'big data applications', such as government surveillance in the fight against terrorism and organized crime.[9] This refers to both the bulk collection and storage of personal data as well as the subsequent combination of this data—stemming from multiple sources—with a view to their analysis and cross-referencing using computer algorithms, i.e., 'big data analytics'.[10]

This ability to "create information about data that were never apparent or intended in the source information"[11] is yin and yang: on the one hand, the predictive potential of big data is particularly valuable for safeguarding national security and preventing crime.[12] Hence, it is recognized that governments may need to resort to new technologies in order to identify and obviate new threats, "including mass surveillance of communications."[13]

Indeed, communications data arguably paint the most comprehensive picture of an individual's private life, especially since the advent of the Web 2.0 era and Social Networking Services.[14] Consequently, the activities of electronic communication service providers (ECSPs) in particular have been the subject of both specific regulation[15] and considerable controversy.[16]

On the other hand, it is hard to comprehend how these secondary uses can be compatible not only with the principles of purpose limitation and data minimization,[17] which would entail that communication service providers (CSPs) only collect and process personal data that is strictly necessary for the provision of services,[18] but also with the principle of transparency.[19] Moreover, such repurposing undermines the right to informational self-determination, by virtue of which individuals should be able to consent to how and if their personal data should be processed, especially when combined.[20]

And yet, neither the European Union nor the Council of Europe expressly regulate the phenomenon of big data.[21] In these circumstances, it is the two Courts—ramparts of democracy in Europe—which, for now, assume this task.

However, the rights to privacy and to the protection of personal data are not absolute,[22] and thus may be restricted when a higher right is at stake, provided that such a restriction meets the quasi-identical conditions required by the ECHR and the EU Charter.[23]

---

7 Namely, information that relates to an identified or identifiable individual. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR), Article 4(1); Convention 108+ (n 1), Article 2(a).

8 GDPR, Article 4(2); Convention 108+, Article 2(2) and (3).

9 European Data Protection Supervisor, *Opinion 7/2015 on meeting the challenges of big data* (2015), 7.

10 *Ibid*., 7; Council of Europe, Consultative Committee of Convention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (2017) T-PD(2017)01 (COE Big Data Guidelines), 2.

11 Privacy International UK, 'Big Data: Industrial Raw Material', *An Introduction to Data Protection: The EDRi Papers*, Issue 06 [2013], 10.

12 Opinion 7/2015 (n 9), 8; COE Big Data Guidelines (n 10), 1.

13 *Szabó and Vissy v Hungary* App no 37138/14 [2016] ECLI:CE:ECHR:2016:0112JUD003713814, para 68. See also, *Tele2* (n 31), para 103.

14 European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users* (2020) Version 1.0.

15 For example, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37. See also the EU Commission's Proposal COM(2017) 10 final, repealing this Directive.

16 For example, following Edward Snowden's revelations in 2013 concerning the surveillance of electronic communications carried out by US and UK intelligence agencies. Also, the Cambridge Analytica 2018 scandal concerning the use of 'social media targeting' for election manipulation.

17 GDPR (n 7), Article 5(1)(b) and (c); Convention 108+ (n 1), Article 5(4)(b) and (c).

18 Cf Directive 2002/58/EC (n 15), Recital 26.

19 GDPR, Article 5(1)(a) and Recitals 39 and 66; Convention 108+, Art. 5(4)(a).

20 Opinion 7/2015 (n 9), 8. See also, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* App no 931/13 [2017] ECLI:CE:ECHR:2017:0627JUD000093113, para 137; Opinion of Advocate General Szpunar in *Orange România* (Case C 61/19) [2020] ECLI:EU:C:2020:158, point 36: "the concept of consent allows the data subject concerned to decide for him or herself on the legitimacy of restrictions to his or her right to the protection of personal data."

21 Paul, de Hert. and Juraj, Sajfert. (2019). Regulating big data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective, *European Data Protection Law Review*. 5(3), 338-351, 343.

22 Parliamentary Assembly of the Council of Europe, *Resolution 1165 on the right to privacy* (1998), point 11; *Privacy International* (n 29), para 63.

23 ECHR (n 3), Article 8(2); EU Charter (n 5), Article 52(1). Essentially, the restriction must have a basis in law, be necessary, and pursue a verifiable objective of public interest.

Notwithstanding, the Court of Justice of the European Union (CJEU) is free to provide a more comprehensive protection of the rights to privacy and data protection than offered by the European Court of Human Rights (ECtHR) in its interpretation of Article 8 ECHR.[24]

Recently, it has been in the context of government surveillance of communications that the two Courts have been obliged to declare their respective positions regarding the issue of big data applications. More specifically, the Courts have been confronted with the issue of national legislation creating an obligation for CSPs to generally and indiscriminately retain and/or make available the personal data generated by the totality of their users, so that certain competent authorities may subsequently access such data.

Subsequently, it would appear, despite their methodological similarities, that the Courts do not see eye-to-eye when it comes to the latitude afforded to States regarding their choice of surveillance regime (Section 2), nor in terms of their rigor when requiring certain safeguards (Section 3).

2. Views on bulk processing regimes: The thin blue line

The mere existence of legislation providing for the secret surveillance of communications constitutes an interference with the right to privacy of the individuals that fall within its scope.[25]

However, both Convention 108+[26] and the GDPR[27] advocate 'technological neutrality', which should in theory exclude a prohibition on the use of big data applications.[28] Subsequently, one could presume that the ECtHR and the CJEU should also maintain a 'technologically neutral' interpretation of data processing, such that states should have sufficiently large discretion vis-à-vis the techniques to be used for surveillance purposes.

Recent decisions, principally concerning traffic and location data—i.e. the 'who', 'when', 'where', and 'how' of a communication -,[29] have given the Courts the opportunity to clarify their position regarding the bulk processing of data in the context of secret surveillance.

A. To target or not to target? A contrasting advocacy: Since 2014,[30] the CJEU has relentlessly promoted "targeted" regimes of data retention, and thereby emphasized the need for a relationship between the data retained and the supposed threat that the national authorities need to quash.[31]

Likewise, national legislation that would require ECSPs to generally and indiscriminately disclose the traffic and location data relating to all of their subscribers and users to the state's security and intelligence agencies is prohibited, as it exceeds the limits of what is strictly necessary in a democratic society.[32]

The CJEU holds therefore that the order to retain[33] or to grant access to national authorities[34] must be based on "objective criteria" that could establish any connection, "indirect or remote",[35] between the data subsequently retained and/or accessed and the objective of general interest pursued.

For example, in the context of the fight against serious crime, a connection could be demonstrated by the link between the data retained and either: a time period and/or geographical area and/or a group of persons likely to be involved in a serious crime; or persons who could "for other reasons" contribute, through the retention of their data, to

---

24 EU Charter, Article 52(3). See also *Tele2* (n 31), para 129.

25 *Weber and Saravia v Germany* App no 54934/00 [2006] ECHR 1173, para 78.

26 Council of Europe, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No 223* (2018) (COE Explanatory Report), para 2.

27 (n 7) Recital 15.

28 Hert and Sajfert (n 21), 344.

29 *Big Brother Watch and Others v The UK* App nos 58170/13, 62322/14 and 24960/15 [2018] ECLI:CE:ECHR:2018:0913JUD005817013 (*BBW*), para 348; Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790, para 23.

30 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Others and Settinger and Others* [2014] ECLI:EU:C:2014:238.

31 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] EU:C:2016:970, para 106, applying the findings of *Digital Rights Ireland* (see para 59) to national legislation.

32 *Privacy International* (n 29), para 81.

33 Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and Others* and *Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791, para 133.

34 *Privacy International*, para 78.

35 *Privacy International*, para 80; *La Quadrature du Net* (n 33), para 143.

this fight.[36] Likewise, the interference should be limited to specific means of communication,[37] supposedly those that could objectively be considered as strictly necessary in the fight against serious crime; such means were not, however, specified by the CJEU. Internet? Email? Some clarification may be found in Advocate General Campos Sánchez-Bordona's opinion in Ordre des barreaux francophones et germanophone and Others:[38] in this respect, the size of the provider could be taken into account, "highly specialized services" thus being excluded.

A recently elucidated enigma, on the other hand, was what a geographical area with a "high risk" of preparation for or commission of serious crimes might look like,[39] the CJEU giving the example of places that regularly receive a very high volume of visitors or "strategic" locations.[40] Consequently, the order to retain or to grant access to the personal data of persons visiting airports and stations, for example, is justifiable. One may infer a reference to the March 2016 orchestrated bombings of Zaventem Airport and Maalbeek metro station in Brussels that took place just nine months before the Tele2 decision.

These qualifying criteria of 'targeted' processing are unfortunately vague: in giving Member States such leeway in determining an already indirect link between the data retained and the risk posed by the data subject, the risk of abuse is still present. Moreover, as pointed out by the Advocate General,[41] relying on such limited criteria may prove to be a source of discrimination.

On the other hand, for the ECtHR, bulk interception and retention of communications data do not, per se, violate the right to privacy.[42] Indeed, the choice between the two falls within the State's wide margin of appreciation in choosing the appropriate means to achieve the legitimate aim pursued.[43] Consequently, the ECtHR refuses to align itself with the afore described position of the CJEU and require that only communications relating to individuals demonstrating a "reasonable" link with the aim pursued by the surveillance be intercepted[44] as such requirements are incompatible with the very efficiency of such a regime. On the contrary, the ECtHR 'adapts' its minimum safeguards to the regime of bulk interception;[45] however, it would appear that such accommodation is only afforded when national security interests "exclusively" are at stake.[46]

According to the ECtHR, if it's true that targeting results in the interception of a more limited set of personal data, this is not the case at the examination stage where the majority of, if not all the intercepted communications will be analyzed.[47] The result is however reversed in the context of bulk interception, whereby "the discretion to intercept is broader, but stricter controls will be applied at the selection for examination stage", in order of relevancy to the aim pursued.[48] Therefore, both "have the potential to be abused"; it all depends on whether the powers of the competent authorities are clearly defined by the law.[49]

The ECtHR therefore considers the analysis of personal data to constitute a more serious interference than its collection.[50] Indeed, it's in the context of big data analytics that the fundamental issue of 'profiling' arises.

B. Through the looking-glass: the protection afforded to the content of communications: In principle, only the sender and addressee of communications should be aware of their content, to the exclusion of third parties, including the service provider.[51]

The problem with general and indiscriminate interception or retention of communications data is that, inherently, the majority of personal data acquired is unlikely to be relevant for achieving the aim pursued, no matter how legitimate it may be.

---

36 *Tele2* (n 31), para 106; *La Quadrature du Net*, para 144.

37 *Tele2*, para 108; *La Quadrature du Net*, para 147.

38 (Case C-520/18) [2020] ECLI:EU:C:2020:7, point 92.

39 *Tele2 Sverige* (n 31), para 111; *La Quadrature du Net* (n 33), para 150.

40 *La Quadrature du Net*, para 150.

41 Opinion ECLI:EU:C:2020:7 (n 38), point 74.

42 *BBW* (n 29), para 316.

43 *Centrum för Rättvisa v Sweden* App no 35252/08 [2018] ECLI:CE:ECHR:2018:0619JUD003525208, para 112; *BBW*, para 317.

44 *BBW* (n 29), paras 316-17.

45 *Ibid*. para 320.

46 *Centrum för Rättvisa* (n 43), para 114. However, there is an incongruity as the prevention of serious crime was also pursued by the contested legislation in *BBW*.

47 *BBW*, para 329.

48 *Ibid*.

49 *Centrum för Rättvisa* para 113; *BBW*, para 315.

50 See, to the contrary, Opinion of AG Campos Sánchez-Bordona in C 520/18 (n 38), point 75.

51 European Data Protection Supervisor, *Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications* (2017), 9.

This is particularly an issue when sensitive data is indirectly swept up in the mêlée[52] as such data is expressly afforded special, higher protection; its processing normally requiring the explicit consent of the data subject.[53]

The CJEU holds that generalized access to the content of communications, i.e., what was said or written, undermines the very "essence" of the rights to privacy and data protection;[54] in other words, this type of invasive interference would reduce these rights to nothing more than meaningless words. It cannot be saved by an assessment of its proportionality or its pursuit of an objective of general interest.[55] It remains that this respect of the 'essence' criterion is specific to the EU Charter[56] and does not have an equivalent disposition in the ECHR. A contrario, we could presume that targeted access to content may, exceptionally, be allowed.

However, the CJEU has emphasized that, when traffic and location data is generally and indiscriminately retained or transmitted,[57] such that "precise conclusions [may be] drawn concerning the private lives" of the concerned data subjects, the information thusly acquired must be seen as "no less sensitive" than the actual content of communications.[58]

This refers to the technique known as 'profiling', whereby combined sets of personal data are made subject to automated processing and analysis in order to make predictions about and decisions regarding the concerned data subject.[59]

Nonetheless, even in these circumstances, if the content isn't affected, for the CJEU, the 'essence' of these rights is preserved.[60] One could see in such a conclusion the reluctance of the Court to completely rule out big data applications, of which the efficiency relies mainly upon the collection of 'observed' or 'inferred' data in order to detect behavioral patterns.[61]

The ECtHR on the other hand, although it considers the acquisition of the content of communications to constitute a particularly intrusive interference, affords—as it would appear from its most recent case-law—the corresponding metadata the same level of protection.[62] Apparently, the content wouldn't necessarily contain more sensitive information. On the contrary, traffic and location data, especially when acquired in bulk, can often reveal more about an individual's private life than the sometimes incredibly insipid content of the communications themselves, such as daily movements, social relationships, or even sensitive information such as religious conviction or state of health.[63]

It would thus appear that the ECtHR took the CJEU's reasoning and ran with it, avoiding the "arbitrary and irrelevant"[64] 'essence' criterion.

This approach is to be preferred as the protection it affords is more adapted to the digital era where electronic devices, often associated with online identifiers—such as internet protocol addresses, cookie identifiers, GPS tracking[65] -, allow for the recording of information on both the users and their environment[66] which, albeit mundane in itself, when combined with actively provided information, paints a much clearer picture of the data subject.[67]

---

52 Opinion 7/2015 (n 9), 7. See, for example, *L.H. v Latvia* App no 52019/07 [2014] ECLI:CE:ECHR:2014:0429JUD005201907, in which the law failed to limit the scope of personal data that could be collected such that medical data was collected.

53 GDPR (n 7), Article 9 and Recital 51; Convention 108+ (n 1), Article 6.

54 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 94; *Tele2* (n 31), para 101.

55 European Union Agency for Fundamental Rights and Council of Europe, 'Modern challenges in personal data protection', *Handbook on European data protection law* (2018), 44.

56 (n 5) Article 52(1).

57 NB General and indiscriminate transmission of bulk communications data to national authorities is equivalent to general access (see *Privacy International* (n 29), paras 79-80).

58 *Privacy International*, para 71; *La Quadrature du Net* (n 33), paras 117-119.

59 Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (2018) WP 251rev.01, 7.

60 *Tele2 Sverige* (n 31), para 101.

61 Opinion 7/2015 (n 9), 10.

62 *BBW* (n 29), paras 356-57. Indeed, this conclusion must be inferred, as the Court found that the safeguards applied to the content of communications should also be applied to the examination of related data.

63 *Ibid*. Cf *La Quadrature du Net* (n 33), para 117.

64 With reference to European Digital Rights' submissions in *BBW* (para 301).

65 GDPR (n 7), Recital 30.

66 European Commission, 'Advancing the Internet of Things in Europe' (2016) SWD(2016)110, para 1.1.

67 Guidelines 8/2020 (n 14), 4-5.

3. The 'European essential guarantees':[68] the scale of legitimacy

There is no denying that the safeguarding of national security and the prevention of crime constitute justifiable restrictions on the rights to privacy and the protection of personal data.[69]

Rather, it's the safeguards provided for by national legislation that come within the firing line of the Courts' scrutiny. To this effect, the European Data Protection Board recommends that the CJEU align itself with the ECtHR,[70] which takes into consideration the combination of safeguards in place, rather than assessing them independently.[71] This 'compensation' principle does not, however, seem to have the favor of the CJEU.

Both Courts recognize that safeguards are all the more indispensable in the context of automatic processing.[72] Indeed, computer algorithms can advance "spurious correlations in data, even in cases where there is no direct cause and effect between two phenomena that show a close correlation," which may result in discrimination.[73] Even so, automatic processing is central in big data applications.

Traditionally, restrictions upon the rights to privacy and data protection are admitted in so far as they prove to be strictly necessary in a democratic society.[74]

To this end, the law must clearly define in what circumstances and under which conditions the retention of[75] or access to[76] communications data may be ordered. However, this definition need not be exhaustive.[77] Indeed, threats to national security are metamorphic;[78] the competent authorities must therefore have sufficient flexibility in order to be able to uncover "previously unknown threats."[79]

This flexibility is however a reflection of the aim pursued; to this effect, neither all aims nor all safeguards are created equal in the eyes of the Courts.

A. Bulk processing of data: the antithesis of proportionality?: As a general rule, the Courts examine whether the seriousness of the interference can be justified by the importance, the 'legitimacy' of the aim pursued.[80]

Therefore, bulk retention or interception of communications data and, a fortiori, its general and indiscriminate subjection to automatic processing—comprehensiveness being the antithesis of proportionality -, should be excluded.

However, the CJEU has acknowledged that the protection of national security is a case apart, capable of justifying more serious interferences with the rights to privacy and data protection.[81]

Therefore, the general and indiscriminate retention of traffic and location data pertaining to all users of electronic communication services is exceptionally possible, provided that it can be "sufficiently" demonstrated that there is a serious and genuine threat, which can be present or foreseeable, to national security.[82] In a desperate attempt to remain coherent in its advocacy of targeted processing, the CJEU states that the very existence of the threat is "in itself" the link between the data subjects and the interference with their rights.[83] However, the retention cannot be indefinite or systematic; it is only lawful where it is limited in time and to what is strictly necessary[84] and where it has been authorized

---

68 Article 29 Data Protection Working Party, *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data* (2016) WP237.

69 See texts cited at footnote 23. See also, GDPR (n 7), Article 23(1)(a) and (d); Convention 108+ (n 1), Article 11(1)(a).

70 European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures* (2020), 15.

71 *Kennedy v The UK* App no 26839/05 [2010] ECHR 682, para 153.

72 *S and Marper* (n 4), para 103; *Digital Rights Ireland* (n 30), para 55.

73 Opinion 7/2015 (n 9), 8.

74 Although the terminology "strictly necessary" is more particular to the CJEU, the ECtHR nevertheless acknowledges that there are "stricter" standards required in the context of surveillance of telecommunications, considered to interfere more with the right to privacy than other interferences. See *Uzun v Germany* App no 35623/05 [2010] ECHR 2263, para 66.

75 *Tele2* (n 31), para 109; *La Quadrature du Net* (n 33), para 132.

76 *Tele2*, para 118; *Privacy International* (n 29), para 68. *BBW* (n 29), para 328.

77 See for example *Kennedy v The UK* (n 71), para 159.

78 *Roman Zakharov v Russia* App no 47143/06 [2015] ECLI:CE:ECHR:2015:1204JUD004714306, para 247.

79 Opinion of Advocate General Campos Sánchez-Bordona in *Privacy International* (Case C-623/17) [2020] ECLI:EU:C:2020:5, point 20. See also, *Szabó and Vissy* (n 13), para 64.

80 *Segerstedt-Wiberg and Others v Sweden* App no 62332/00 [2006] ECHR 597, para 88; Case C 207/16 *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788, para 55.

81 *Privacy International* (n 29), para 75; *La Quadrature du Net* (n 33), para 136.

82 *La Quadrature du Net*, para 137.

83 *Ibid*.

beforehand by a court or an independent administrative body whose decision is binding.[85] The same goes for the automated analysis of such data.[86]

Other objectives of general interest, such as the prevention and prosecution of crimes, although legitimate, would therefore afford the legislator less discretion in its ability to impose bulk retention obligations on CSPs.

Consequently, the serious interferences that represent, on the one hand, the legal obligation imposed on ECSPs to retain the traffic and location data of their subscribers and users,[87] and, on the other hand, legislation that obliges ECSPs to grant the competent national authorities access to such retained data,[88] can only be justified by the pursuit of combating serious crime. On the other hand, in the same context, where the access by public authorities to retained data is not deemed to be serious, such an interference can be justified by the objective of fighting crime in general.[89]

An interesting comparison is to be drawn with the recent decision Breyer v Germany.[90] In this case, only subscriber data was concerned. The retained data was thus "limited," concerning less intrusive information – namely telephone numbers, names and addresses, dates of birth, and date of the contracts[91]—than that which is provided by traffic and location data which "allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned," or than the "highly personal information" which is revealed by the content of communications.[92]

Therefore, the ECtHR found that the link was not to be made between the case at hand and Tele2[93] which—although it also concerned a general obligation of retention covering all subscribers and users of telecommunication services[94] who, as pointed out by the applicants,[95] were, at face value, neither suspected of being involved in criminal activities nor presenting a threat for public safety[96] -, dealt with traffic and location data. Rather, the link was to be made with Ministerio Fiscal, which also concerned subscriber data.[97]

In this regard, for the ECtHR, proportionality must be assessed, and the required rigor of the safeguards determined, not only with regard to the quantity of the personal data processed, but also its quality, i.e., the diversity of information processed,[98] such that 'low quality' data—like subscriber data—may be retained and made available to national authorities in bulk without constituting a disproportionate interference with the right to privacy. Confusing, as, in the same breath, the ECtHR states that "in view of the possibilities of processing and combining, there is no item of personal data which is in itself, that is, regardless of the context of its use, insignificant."[99]

Judge Ranzoni's dismissal[100] of the comparison made between Ministerio Fiscal and Breyer was, in this respect, justified, with regard to some substantial differences. In Ministerio Fiscal, the interference was limited to specific sets of subscriber data that were relevant to the elucidation of a specific crime, namely data relating only to the telephone numbers corresponding to SIM cards activated with the stolen mobile phone and to the identity of the owners of those cards. Thus an objective of fighting non-serious crime was justified.[101] Whereas, in Breyer, the measure of retention was general and preventative in nature, concerning the subscriber data of all users of telecommunication services. Consequently, pursuant to the CJEU's case-law, only the fight against serious crime or the protection of national security should have justified such a measure. This was not, however, the case: the measure's purpose was, on the contrary, to facilitate, inter alia, the prosecution of criminal offences in general and the performance of intelligence duties.[102] This was where Judge Ranzoni's criticism lay.[103]

---

84 *Ibid*. para 138.
85 *Ibid*. para 139.
86 *Ibid*. paras 174-79.
87 *Tele2* (n 31), paras 102-03.
88 *Ibid*. paras 115-16.
89 *Ministerio Fiscal* (n 80), para 57.
90 App no 50001/12 [2020] ECLI:CE:ECHR:2020:0130JUD005000112.
91 *Ibid*. para 61.
92 *Ibid.* paras 92-94. Cf *Ministerio Fiscal*, para 60.
93 (n 31) para 105.
94 *Breyer* (n 90), para 93.
95 *Ibid*. para 67.
96 Ie the legitimate aims pursued by the contested legislation (*ibid*. para 86).
97 *Ibid*. para 94.
98 Cf COE Explanatory Report (n 26), para 52. See also Dissenting opinion of Judge Ranzoni in *Breyer* (n 90), point 11.
99 *Breyer*, para 81, citing the German Federal Constitutional Court.
100 Dissenting opinion (n 98), point 13.
101 *Ministerio Fiscal* (n 80), paras 59-61.
102 *Ibid*. para 87.
103 Dissenting opinion in *Breyer* (n 98), point 3.

B. An opposing view of 'minimality': the need for independent prior review: Secret surveillance, especially when pursuing 'broadly formulated threats' such as those to national security,[104] is inherently liberticide; the risk is that it may undermine democracy "under the cloak of defending it."[105] Hence, the need for supervision by an independent and impartial third party, judicial control epitomizing such a task.[106]

Ex ante review, in other words authorization, objectively offers the best guarantees for data subjects. Indeed, at this stage, no interference with their rights has yet occurred; moreover, surveillance will only be possible if the competent authority deems it to be strictly necessary.

Providing for such independent prior review is seen as mitigating, at least, the initial lack of notification of the data subject, inherent to the very nature of surveillance regimes, i.e., secrecy,[107] and in practice impossible in the context of bulk interception and retention of communications, where there are no clearly defined surveillance targets.[108]

This is where the courts seem to differ.

Recently, in the context of processing bulk communications data for surveillance purposes, the ECtHR emphasized that, if it recognizes that prior judicial authorization is certainly an "important safeguard"[109] and even "desirable,"[110] it does not impose it as a minimum safeguard; in itself, it is neither necessary nor sufficient to ensure compliance with Article 8 of the ECHR.[111] On the contrary, the ECtHR even appears to argue against authorization, implying that even judges—the guardians of liberty—cannot provide iron-clad protection from abuse for data subjects.[112] However, there should be "extensive" judicial supervision present for the subsequent duration of the surveillance regime.[113]

The CJEU's position in the matter couldn't be more different. Firstly, the ECtHR's use of "desirable"[114] is in clear contrast to the "essential" of the CJEU. In Tele2, the CJEU ruled that where 'vital' national security interests are jeopardized, general access to bulk retained traffic and location data—or, in the context of serious crime, access limited to the data of users suspected of being directly or indirectly involved[115]—is exceptionally possible. However, it is "essential" that, except in cases of "validly established urgency,"[116] such access has been authorized by a court or by an independent administrative body.[117] The 'essentiality' of prior review was reiterated in la Quadrature du Net, this time regarding both the general and indiscriminate retention of traffic and location data by ECSPs where there is a serious threat to national security[118] as well as the real-time collection of traffic and location data by national authorities in the context of preventing terrorism.[119] The decision of the reviewing authority must, furthermore, be "binding."[120]

As pointed out by Judge Koskelo,[121] the ECtHR has held this position for almost four decades, whilst technology has undergone innumerable mutations in half of that time; and yet the Court's reasoning has not evolved concomitantly. Besides, it is difficult to see how the Court could argue that judicial authorization could unreasonably impede the efficiency of secret surveillance regimes; if the interference isn't deemed necessary by the judge or other competent authority, it shouldn't be carried out in the first place. Arguably, the ECtHR is here playing 'facilitator' and not 'guardian of efficiency'.

---

104 Joint partly dissenting and partly concurring opinion of Judge Koskelo, joined by Judge Turkoviæ in *BBW* (n 29), point 14.

105 *Roman Zakharov* (n 78), para 232.

106 *Ibid*. para 233.

107 *Centrum för Rättvisa* (n 43), paras 106, 164-67; *BBW* (n 29), para 310.

108 *BBW*, para 317.

109 *Centrum för Rättvisa*, para 133; *BBW*, para 320.

110 *BBW*, para 376.

111 *Centrum för Rättvisa*, para 133; *BBW*, para 320.

112 *BBW*, para 319.

113 *Centrum för Rättvisa*, para 133, referring to *Szabó and Vissy* (n 13), para 77.

114 *BBW*, para 376.

115 *Tele2* (n 31) para 119. Cf *Roman Zakharov* (n 78), para 260.

116 *Ibid*. para 120. Cf *Szabó and Vissy* (n 13), paras 80-81, wherein the Court accepted that in situations of extreme urgency, such judicial authorization could waste "precious time," such that a post factum judicial review would suffice.

117 *Ibid*. paras 119-20. Cf *Szabó and Vissy* (n 13), para 73, which emphasizes the need for a judge to verify both strict necessity and exoneratory circumstances of urgency.

118 *La Quadrature du Net* (n 33), para 139.

119 *Ibid*. para 189.

120 Cf *Roman Zakharov* (n 78), para 263.

121 Opinion in *BBW* (n 104), points 20-29.

4. Conclusion

As duly pointed out by the Judges Pardalos and Eicke in their dissenting opinion,[122] the CJEU appears to have adopted a more prescriptive approach regarding the safeguards it considers necessary. This was demonstrated, for example, by the fact that, in Privacy International, the referring court only doubted the compatibility of UK legislation with the 'Tele2 requirements', as opposed to those imposed by the ECtHR in application of Article 8 of the ECHR.[123]

Is there nevertheless a possibility, in the cases under appeal,[124] that the Grand Chamber will align itself with the CJEU? Unlikely, given that the latter's most recent decisions, as earlier explored, serve largely as confirmation of their antecedents, which were already infamous by the time the lower sections of the ECtHR had rendered their decisions.

Perhaps the CJEU's dogmatism owes to the fact that personal data protection is recognized as a distinct right within the European Union.[125] However, this would be an over-simplification of the debate.

Notwithstanding, the CJEU's position is welcome, albeit lacking in clarity. In the context of bulk processing, it is undesirable to systematically put the need for authorities to effectively perform their police and/or intelligence duties before the protection of personal data, especially when the outcome of this balancing act is based upon the 'quality' of the data, an arguably subjective criterion.

Indeed, the regulation of data protection is more than "just a matter of volume."[126] Technology, and the capacities it gives us in terms of communication, has become an intrinsic part of our lives. The extent to which we expose the core of our private sphere has intensified; the 'data policies' of ECSPs in particular do not truly reflect this reality.

Big data applications aren't going anywhere; on the contrary. A recent example is the government monitoring of the Covid-19 pandemic via contact tracing smartphone applications. Many experts were quick to sound the alarm on the dangers of fresh-out-of-the-oven apps and their mass processing of personal data (predominantly location data), principally collected by mobile-telecommunication service providers;[127] their main concerns being the repurposing of such data for law-enforcement purposes or the formation of centralized databases that would remain at the disposal of national authorities beyond the evanescence of the pandemic.[128]

The European Data Protection Board emphasized the need to limit the collection of data to what was strictly necessary to halt the spread of the virus.[129] One wonders how information on an individual's sexual partners could have been justified in this context.[130]

---

122 In *BBW* (n 29), point 22.

123 Opinion ECLI:EU:C:2020:5 (n 79), point 18.

124 Namely *Centrum för Rättvisa* (n 43) and *BBW*.

125 Such that, if an act of processing personal data may interfere with the right to privacy, it will always engage the right to data protection: see *Handbook on European data protection law* (n 55), 19-20.

126 Opinion of Judge Koskelo in *BBW* (n 104), point 12.

127 European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* (2020), 4.

128 Ada Lovelace Institute, *COVID-19 Rapid evidence review: Exit through the App Store?* (8 April 2020); Guidelines 04/2020 (n 127), 7-8.

129 European Data Protection Board, *Statement on the processing of personal data in the context of the COVID-19 outbreak* (2020), 3.

130 Regarding the NHS' Test-and-Trace system. https://www.bbc.co.uk/news/explainers-52442754 accessed 20 November 2020.

Cite this article as: Heather Taylor (2021). Data protection in a European world of ideals: An unforeseeable division of camps. *International Journal of Data Science and Big Data Analytics.* 1(2), 14-22. doi: 10.51483/IJDSBDA.1.2.2021.14-22